ECSE 416 – Intro to Telecom Networks – Fall 2020
Test 1
Sept. 21, 2020
Due Friday Sept. 25th midnight. Please scan your answers and submit the scanned pages as a single pdf file. Alternatively, you can prepare answers in electronic format and submit a single pdf.
3 questions, 60 marks

There are 3 questions. Marks allocated to each part are indicated in square brackets.

This exam is **open book**. You are permitted to consult any resources — textbook, web, notes. But do not discuss the questions and solutions with your classmates. Do not ask anyone else to help you solve the problems.

Question 1 [20 marks]

Inspired by the fintech boom (although a little late to the party), Markus Misguided decides to create an online money payment service similar to PayPal.

His service, PayMe, allows users to transfer money to other users of the system. To ensure that no fraudulent activity takes places, the service issues a pair of keys (public and private) to each user. If Alice ("A") wishes to give X dollars to Bob ("B"), she sends the following message to the PayMe service ("S"):

$$A \rightarrow S : A, B, X, n, \{X|n\}_{A^-} \tag{1}$$

where n is a nonce created by Alice, A^- is Alice's private key, and $\{M\}_{K^-}$ denotes a digital signature over M computed using the private key K^-. This notation says that A, B, X and n are transmitted in plaintext. Then the concatenation of X and n is encrypted using Alice's private key and transmitted.

a) Is the PayMe scheme secure? To what attack is it vulnerable? And if it is vulnerable, how can it be fixed?

b) Consider a scenario where Alice accesses a website using an http session to buy shoes. The payment page says "Please click here to access the PayMe service. Please transfer $242.50 via PayMe to SpendLessShoes and we will then ship your order to you." If Trudy can intercept this http session, what attack could she execute? Would this attack be successful even after your modification to the PayMe scheme in part a)? Describe how you could modify the payment process on the website to avoid such an attack. Make sure that you clearly explain how you have removed the vulnerability.

Question 2 [20 marks]

You are the administrator of a 220.220.0/24 network. You have a gateway available that has 4 configurable interfaces - `br0`, `br1`, `eth0` and `lo`. The first two, `br0` and `br1`, are internal interfaces. These can be used to split the network into two subnets, and to allow for different rules to be applied to different user groups.

You have 160 users in total and you want to provide an internal webserver that is only available to 100 special users in your network. You also want to provide a second webserver that is accessible to all users, both internal to your network and external. Finally, you would like to block all outgoing UDP traffic.

a) Provide the iptables instructions that would configure a firewall at the gateway to achieve these goals. Provide an illustration of your network, clearly indicating the interfaces and the allocated IP spaces (i.e. the subnets). Identify the IP addresses associated with the users with privileged access.

b) You learn about the Code Red worm and you curse yourself because you've been too lazy to patch your IIS server. Luckily it hasn't been infected yet. You could just pull the plug but the users who are running other jobs on the server would be livid. So you type furiously to reconfigure your firewall to give yourself some time to apply the patch. What do you type?

Question 3 [20 marks]

The first version of the Code Red worm (Code Red v1) accidentally used the same random seed for every thread and every new instance of the worm. As a result each thread and instance scanned exactly the same hosts.

Suppose Code Red v1 allocated 10s to scan each new candidate host (sending the TCP connection request and waiting for a response or a timeout). If the scan was successful, the 10s includes the infection time. Let us assume that 2 million webservers were vulnerable.

The second version of the Code Red worm used random seeds and 100 threads for each machine.

a) With this process, for the first misconfigured Code Red v1 worm, how long did it take on average before the first new susceptible host was identified and infected?

b) How long did it take, on average, before 1000 webservers were infected by Code Red v1? What about 10,000? In your calculations, you can ignore the reduction in the 2 million susceptible hosts.

c) How long did it take, on average, for the 100 threads of Code Red v2 to find and infect the first vulnerable server?

d) How long did it take, on average, to infect the first 1000 servers? The first 10,000? As before, you can ignore the reduction in the susceptible population.